Dr. Jorge Vitória
Università degli Studi di Cagliari, 2020/2021
Corso di Laurea in Matematica

Esercizi per il Corso di ALGEBRA 2 - PARTE 2

Foglio 4

21 maggio 2021

Prima degli esercizi, dimostriamo il seguenti teorema (alcuni passaggi sono lasciati come esercizio!).

Teorema 1.31. *Sia A un dominio fattoriale. Allora $A[x]$ è un dominio fattoriale.*

Dimostrazione: Sia A un dominio fattoriale e $\mathbb{K}$ il suo campo di quozienti. Dimostriamo che ogni polinomio f in $A[x]$ si fattorizza (in modo unico a meno di ordine e associazione) come prodotto di elementi irriducibili in $A[x]$ per induzione su $n = \mathsf{deg}(f)$.
Se $n = 0$, allora f è costante e, siccome A è un dominio fattoriali, $f = a_1 \cdots a_n$ dove $a_1, \cdots, a_n$ sono elementi irriducibili in A. Ogni elemento irriducibile in A è anche irriducibile in $A[x]$ **(esercizio!)** e, allora, questa è una fattorizzazione di f come prodotto di elementi irriducibili in $A[x]$. La fattorizzazione è unica a meno di ordine e associazione in A e, dato che $U(A[x]) = U(A)$ e che ogni fattorizzazione di f è necessariamente un prodotto di elementi di grado 0, concludiamo che questa fattorizzazione è unica a meno di ordine e associazione in $A[x]$.
Supponiamo adesso che la esistenza di una tale fattorizzazione è vera per polinomi di grado minore di n, e sia f un polinomio di grado n. Scriviamo $f = \mathsf{cont}(f) f_1$ dove f_1 è primitivo. Siccome A è un dominio fattoriale, $\mathsf{cont}(f) = a_1 \cdots a_n$ dove $a_1, \cdots a_n$ sono elementi irriducibili in A (e, quindi, in $A[x]$). Se f_1 è irriducibile in $A[x]$, allora abbiamo trovato una fattorizzazione di f come prodotto di elementi irriducibili, e questa fattorizzazione è unica a meno di ordine e associazione **(esercizio!)**. Se f_1 non è irriducibile, allora $f_1 = gh$ dove $n > \mathsf{deg}(g) > 1$ e $n > \mathsf{deg}(h) > 1$ **(esercizio!)**. Per ipotesi induttiva, abbiamo allora che g e h si possono scrivere come prodotti di elementi irriducibili. Di conseguenza otteniamo una fattorizzazione di f come prodotto di elementi irreducibili.
Nella dimostrazione della esistenza di una fattorizzazione di f abbiamo fatto una scelta di come fattorizzare f_1. Nonostante il fatto che g e h si spezzano, per ipotesi induttiva, in modo unico a meno di ordine e associazione dei fattori, questo non è ancora chiaro per f_1 e, di conseguenza, per f. Supponiamo allora che $f = g_1 \cdots g_m = h_1 \cdots h_l$ dove tutti i fattori g_i e h_j sono irriducibili. Siccome $n > 0$, almeno uno dei fattori g_i ha grado > 0, diciamo (senza perdita di generalità, g_1) e consideriamo g_1 come un elemento di $\mathbb{K}[x]$. Dal teorema 1.30, abbiamo che g_1 è irriducibile in $\mathbb{K}[x]$ e, dato che $\mathbb{K}[x]$ è un dominio euclideo, abbiamo che g_1 è primo in $\mathbb{K}[x]$ e, siccome g_1 divide $h_1 \cdots h_l$ in $\mathbb{K}[x]$ **(esercizio!)**, abbiamo che esiste $1 \leq k_1 \leq l$ tale che g_1 divide h_{k_1} in $\mathbb{K}[x]$, cioè, $h_{k_1} = g_1 t_1$ per un certo t_1 in $\mathbb{K}[x]$. Dalla dimostrazione del Teorema 1.30, sappiamo che $t_1 = \frac{a}{b} s_1$ dove a, b sono elementi di A e s_1 è un polinomio primitivo in $A[x]$. Quindi, abbiamo $a g_1 s_1 = b h_{k_1}$ in $A[x]$. Dal Lemma di Gauss, $g_1 s_1$ è primitivo e, siccome h_{k_1} è anche primitivo, concludiamo che a è associato a b in A **(esercizio!)**. Questo ci permette di concludere che $g_1 s_1$ è associato a h_{k_1} in $A[x]$ **(esercizio!)** e, quindi, t_1 è invertibile. Allora questo implica che $g_2 \cdots g_m$ è associato al prodotto degli h_j per $1 \leq j \neq k_1 \leq l$. Abbiamo adesso due fattorizzazioni di un stesso polinomio di grado $< n$ come prodotto di fattori irriducibili. Per ipotesi indutiva, gli fattori sono gli stessi a meno di associazione e ordine. Questo finisce la dimostrazione.

Adesso, ecco gli esercizi!

1. Si dimostri che, dato un polinomio $f = \sum_{i=0}^{n} a_i x^i$ in $\mathbb{Z}[x]$ e $\frac{p}{q}$ una radice di f in $\mathbb{Q}$ con p e q in $\mathbb{Z}$ tali che $\mathsf{mcd}(p, q) = 1$, allora p divide a_0 e q divide a_n.

2. Si fattorizzi il polinomio $f = 4(x^9 - x)$ come un prodotto di elementi irriducibili in $\mathbb{Q}[x]$.

3. Si dimostri che l'estensione di campi $\mathbb{Q} \subseteq \mathbb{R}$ non è finita.

4. Si dimostri che $\mathbb{F} := \mathbb{Q}[x]/\langle x^4 - 5 \rangle$ è un campo, e si trovi l'inverso di $x^2 + 1$ in $\mathbb{F}$.

5. Si dimostri che $\mathbb{Q}(\sqrt{p})$ e $\mathbb{Q}(\sqrt{q})$ non sono campi isomorfi per $p \neq q$ primi positivi in $\mathbb{Z}$.

6. Si dimostri che data un'estensione di campi $\mathbb{K} \subseteq \mathbb{F}$ e dati due elementi a e b in $\mathbb{F}$ che siano algebrici su $\mathbb{K}$, allora gli elementi $a+b$ e ab sono anche algebrici su $\mathbb{K}$.

7. Siano $\mathbb{K} \subseteq \mathbb{F}$ e $\mathbb{F} \subseteq \mathbb{L}$ estensioni di campi. Si dimostri che $\mathbb{L}$ è algebrico su $\mathbb{K}$ se e solo se $\mathbb{L}$ è algebrico su $\mathbb{F}$ e $\mathbb{F}$ è algebrico su $\mathbb{K}$.

8. Si consideri l'elemento $v = \sqrt[3]{2} + \sqrt[3]{4}$ di $\mathbb{R}$;
   (a) Si dimostri che $\mathbb{Q}(v) = \mathbb{Q}(\sqrt[3]{2})$;
   (b) Si trovi il grado di v su $\mathbb{Q}$;
   (c) Si calcoli il polinomio minimo di v su $\mathbb{Q}$.

9. Si consideri l'elemento $u = \sqrt[3]{2}i - 1$ di $\mathbb{C}$.
   (a) Si dimostri che i e $\sqrt[3]{2}$ appartengono a $\mathbb{Q}(u)$;
   (b) Si trovi il grado di $\mathbb{Q}(u)$ su $\mathbb{Q}$;
   (c) Si dimostri che $\mathbb{Q}(u) = \mathbb{Q}(i, \sqrt[3]{2})$;

10. Sia $\mathbb{K} \subseteq \mathbb{F}$ una estensione finita di campi. Si dimostri che se un polinomio f di $\mathbb{K}[x]$ è il polinomio minimo di un elemento a di $\mathbb{F}$, allora il grado di f divide $[\mathbb{F}\colon \mathbb{K}]$.

11. Siano $u = \sqrt{5-\sqrt{5}}$, $v = \sqrt{2+\sqrt{6}}$, $w = \sqrt{3+3\sqrt{2}}$ e $z = \frac{\sqrt[4]{2}}{1+\sqrt{2}}$
   (a) Si calcolino i polinomi minimi di u, v, w e z su $\mathbb{Q}$ e si determinino $[\mathbb{Q}(u) : \mathbb{Q}]$, $[\mathbb{Q}(v) : \mathbb{Q}]$, $[\mathbb{Q}(w) : \mathbb{Q}]$ e $[\mathbb{Q}(z) : \mathbb{Q}]$.
   (b) Si scriva $\frac{1}{u^2}$ come combinazione lineare su $\mathbb{Q}$ di potenze di u.
   (c) Si dimostri che $\mathbb{Q}(z) = \mathbb{Q}(\sqrt[4]{2})$.

12. Sia $\mathbb{S}$ un sottoinsieme di un campo $\mathbb{K}$ tale che $\emptyset \neq \mathbb{S} \neq \{0\}$. Si verifichi che S è un sottocampo di $\mathbb{K}$ se e solo per ogni a e b in S, si ha che $a-b \in \mathbb{S}$ e, se $a \neq 0$ e $b \neq 0$ allora $ab^{-1} \in \mathbb{S}$.

13. Sia $\mathbb{K}$ un campo e f e g due polinomi irriducibili su $\mathbb{K}$. Si dimostri che se esiste un'estensione di campi $\mathbb{K} \subseteq \mathbb{F}$ e $\alpha \in \mathbb{F}$ tali che $f(\alpha) = g(\alpha) = 0$, allora f e g sono associati in $\mathbb{K}[x]$.

14. Sia $\mathbb{F}$ il campo dei quozienti del dominio degli interi di Gauss $\mathbb{Z}[i]$.
   (a) Sia $\mathbb{K}$ un sottocampo di $\mathbb{C}$ tale che $\mathbb{Z}[i] \subseteq \mathbb{K}$. Si dimostri che $\mathbb{F} \subseteq \mathbb{K}$.
   (b) Si dimostri che $\mathbb{F} \cong \mathbb{Q}(i)$.

Inoltre, aggiungo in questo foglio anche gli esercizi relativi alle prossime lezioni!

15. Con l'uso di riga e compasso si costruiscano, a partire di $\{0,1\}$ i seguenti numeri:

$$\text{(a) } \sqrt{7} \qquad \text{(b) } \sqrt{2-\sqrt{2}} \qquad (c) \ \sqrt{\frac{\sqrt{5}+5}{8}}$$

16. Si dimostri che è possibile costruire un pentagono regolare con l'uso di riga e compasso.
   (a) Si osservi che per un numero complesso z di valore assoluto 1, il suo inverso e il suo coniugato concidono. In particolare, si ha che $z + 1/z$ è un numero reale ($2\cos(\theta)$, dove θ è l'argomento di z).
   (b) Si consideri il numero complesso $\omega = \cos(2\pi/5) + i\sin(2\pi/5)$. Si dimostri che

$$\omega^2 + \omega + 1 + \omega^{-1} + \omega^{-2} = 0.$$

(c) Si dimostri che $4\cos^2(2\pi/5)+2\cos(2\pi/5)-1=0$.

(d) Si dimostri che ω è costruibile e che, quindi, è possibile costruire un pentagono regolare con l'uso di riga e compasso.

17. Si dimostri che non è possibile costruire un ettagono regolare con l'uso di riga e compasso.

(a) Si consideri il numero complesso $\omega=\cos(2\pi/7)+i\sin(2\pi/7)$. Si dimostri che

$$\omega^3+\omega^2+\omega+1+\omega^{-1}+\omega^{-2}+\omega^{-3}=0.$$

(b) Si dimostri che $p=8x^3+4x^2-4x-1$ è il polinomio minimo di $\cos(2\pi/7)$ su $\mathbb{Q}$.

(c) Si concluda che ω non è costruibile e che, quindi, non è possibile costruire un ettagono regolare con l'uso di riga e compasso.